



IPW

XA-10074
PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Tsutomu IMAI et al.

Appln. No.: 10/825,674

Group Art Unit: 2186

Filed: April 16, 2004

For: NONVOLATILE MEMORY DEVICE AND DATA PROCESSING SYSTEM

* * *

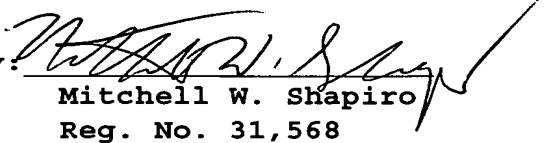
CLAIM OF PRIORITY UNDER 35 U.S.C. § 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby claim the priority of Japanese
Patent Application No. 2003-117822 filed April 23, 2003,
and submit herewith a certified copy of said application.

Respectfully submitted,

By: 
Mitchell W. Shapiro
Reg. No. 31,568

MWS:lat

Miles & Stockbridge P.C.
1751 Pinnacle Drive
Suite 500
McLean, Virginia 22102-3833
(703) 903-9000

July 30, 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

10,825,674

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日 2 0 0 3 年 4 月 2 3 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 1 1 7 8 2 2
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 1 1 7 8 2 2]

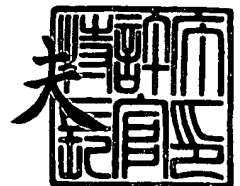
出 願 人 株 式 会 社 ル ネ サ ス テ ク ノ ロ ジ
Applicant(s):

BEST AVAILABLE COPY

2 0 0 4 年 4 月 9 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 2 9 4 7

【書類名】 特許願

【整理番号】 H03004781

【提出日】 平成15年 4月23日

【あて先】 特許庁長官殿

【国際特許分類】 G06K 17/00

【発明者】

 【住所又は居所】 東京都千代田区丸の内二丁目 4 番 1 号 株式会社ルネサ
 ステクノロジ内

 【氏名】 今井 勉

【発明者】

 【住所又は居所】 東京都千代田区丸の内二丁目 4 番 1 号 株式会社ルネサ
 ステクノロジ内

 【氏名】 兼平 晃

【発明者】

 【住所又は居所】 東京都千代田区丸の内二丁目 4 番 1 号 株式会社ルネサ
 ステクノロジ内

 【氏名】 片山 国弘

【特許出願人】

 【識別番号】 503121103

 【氏名又は名称】 株式会社ルネサステクノロジ

【代理人】

 【識別番号】 100089071

 【弁理士】

 【氏名又は名称】 玉村 静世

 【電話番号】 03-5217-3960

【手数料の表示】

 【予納台帳番号】 011040

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 不揮発性記憶装置及びデータ処理装置

【特許請求の範囲】

【請求項 1】 制御回路と不揮発性記憶回路とを有し、

前記不揮発性記憶回路は利用情報に対するアクセス制限を行なう制限情報の格納領域を有し、

前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、

前記制御回路は、外部より供給される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行ない、

前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、

前記制御回路によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なうことを特徴とする不揮発性記憶装置。

【請求項 2】 制御回路と不揮発性記憶回路とを有し、

前記不揮発性記憶回路は利用情報に対するアクセス制限を行なう制限情報の格納領域を有し、

前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、

前記制御回路は、外部より供給される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行ない、

前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、

前記制御回路によるアクセス判定動作を少なくとも不揮発性記憶装置へ動作電源を投入するときと動作電源を遮断するときに行なうことを特徴とする不揮発性

記憶装置。

【請求項 3】 前記不揮発性記憶回路は前記利用情報の格納領域を有し、前記不揮発性記憶装置は前記利用情報を複数に分割してアクセスを行ない、

アクセス開始時の前記アクセス判定動作においてアクセス可と判定された後、分割された前記利用情報のアクセス毎又は所定の複数アクセス毎に前記アクセス判定動作を行なうことを特徴とする請求項 1 又は 2 記載の不揮発性記憶装置。

【請求項 4】 分割された前記利用情報のアクセス単位はセクタであることを特徴とする請求項 3 記載の不揮発性記憶装置。

【請求項 5】 前記分割された利用情報のアクセスに対するアクセス判定動作において、第 2 回目以降のアクセス判定動作では、時刻情報が前記アクセス期限情報により示されるアクセス期限より後であってもアクセス可と判定することを特徴とする請求項 3 記載の不揮発性記憶装置。

【請求項 6】 前記不揮発性記憶装置は前記時刻情報を出力可能な外部装置に接続され使用されるものであり、前記外部装置へ前記分割された利用情報を出力可能であることを特徴とする請求項 3 記載の不揮発性記憶装置。

【請求項 7】 前記不揮発性記憶回路は不揮発性半導体メモリであり、外部装置に接続されるインタフェース端子を有する所定のメモリカードケーシングに内蔵されて成ることを特徴とする請求項 3 記載の不揮発性記憶装置。

【請求項 8】 前記制限情報は前記制御回路により暗号化されて前記不揮発性記憶回路に格納されることを特徴とする請求項 1 又は 2 記載の不揮発性記憶装置。

【請求項 9】 前記制限情報の暗号化に用いる暗号鍵は不揮発性記憶装置固有の属性情報であることを特徴とする請求項 8 記載の不揮発性記憶装置。

【請求項 1 0】 前記制御回路は前記利用情報を復号するためのコンテンツ鍵を含む利用情報ライセンスを受領するために証明情報を外部に出力可能であることを特徴とする請求項 1 又は 2 記載の不揮発性記憶装置。

【請求項 1 1】 前記制御回路は、前記利用情報ライセンスを外部から受領して前記不揮発性記憶回路に格納することを特徴とする請求項 1 0 記載の不揮発性記憶装置。

【請求項 1 2】 前記制御回路は前記コンテンツ鍵とともに入力される時間情報を前記アクセス時間情報の初期値として前記不揮発性記憶回路に格納することを特徴とする請求項 1 1 記載の不揮発性記憶装置。

【請求項 1 3】 前記不揮発性記憶回路はアクセス制限領域とアクセス非制限領域とを有し、

前記制限情報はアクセス制限領域に格納され、

前記利用情報はアクセス非制限領域に格納されることを特徴とする請求項 1 又は 2 記載の不揮発性記憶装置。

【請求項 1 4】 前記制御回路は外部からの認証を受けて前記アクセス制限領域に対する書き込みが可能にされることを特徴とする請求項 1 3 記載の不揮発性記憶装置。

【請求項 1 5】 前記アクセス制限領域は前記利用情報ライセンスの格納領域とされることを特徴とする請求項 1 4 記載の不揮発性記憶装置。

【請求項 1 6】 前記制御回路は外部から与えられる証明情報に対する認証を行なって前記アクセス制限領域に対する読み出しを可能にすることを特徴とする請求項 1 3 又は 1 4 記載の不揮発性記憶装置。

【請求項 1 7】 再生部と利用制限部とを有し、利用情報に対するアクセス制限を行なう制限情報を格納する書換え可能な記憶媒体をアクセスして前記利用情報を再生可能なデータ処理装置であって、

前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、

前記利用制限部は、データ処理装置で生成される時刻情報と前記制限情報とに基づいて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記記憶媒体上の前記アクセス時間情報を更新するアクセス判定動作を行ない、

前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、

前記利用制限部によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なうことを特徴とするデータ処理装置。

【請求項 18】 再生部と利用制限部とを有し、利用情報に対するアクセス制限を行なう制限情報を格納する書換え可能な記憶媒体をアクセスして前記利用情報を再生可能なデータ処理装置であって、

前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、

前記利用制限部は、データ処理装置で生成される時刻情報と前記制限情報とに基づいて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記記憶媒体上の前記アクセス時間情報を更新するアクセス判定動作を行ない、

前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、

前記利用制限部によるアクセス判定動作を少なくとも再生部へ記憶媒体を装着するときと再生部から記憶媒体を離脱するときに行なうことを特徴とするデータ処理装置。

【請求項 19】 前記利用制限部は、再生部に記憶媒体が装着された状態で動作電源が投入されるときと、再生部に記憶媒体が装着された状態で動作電源が遮断されるときに前記アクセス判定動作を行なうことを特徴とする請求項 18 記載のデータ処理装置。

【請求項 20】 前記利用制限部は、記憶媒体固有の属性情報を暗号鍵とする暗号化を行なってアクセス時間情報の更新を行なうことを特徴とする請求項 17 乃至 19 の何れか 1 項記載のデータ処理装置。

【請求項 21】 前記記憶媒体は書換え可能な不揮発性記憶装置であることを特徴とする請求項 17 乃至 19 の何れか 1 項記載のデータ処理装置。

【請求項 22】 前記不揮発性記憶装置はアクセス制限領域とアクセス非制限領域とを有し、

前記利用制限判定部はアクセス制限領域に対して制限情報のアクセスを行ない、

前記再生部はアクセス非制限領域に対して利用情報のアクセスを行なうことを特徴とする請求項 21 記載のデータ処理装置。

【請求項 2 3】 前記利用制限部は不揮発性記憶装置から与えられる証明情報に対して認証を行なった後に前記アクセス制限領域に書き込みが可能にされることを特徴とする請求項 2 2 記載のデータ処理装置。

【請求項 2 4】 前記アクセス制限領域は前記利用情報を復号するための利用情報ライセンスの格納領域とされることを特徴とする請求項 2 3 記載のデータ処理装置。

【請求項 2 5】 前記利用制限部は不揮発性記憶装置に証明情報を与えて認証を受けた後に前記アクセス制限領域に対する読み出しが可能にされることを特徴とする請求項 2 4 記載のデータ処理装置。

【請求項 2 6】 ホストインタフェース制御部を有し、当該ホストインタフェース制御部は、前記利用情報を復号するためのコンテンツ鍵を含む利用情報ライセンスを受領するために前記記憶媒体が保有する証明情報をホスト装置に向けて出力可能であることを特徴とする請求項 1 7 乃至 1 9 の何れか 1 項記載のデータ処理装置。

【請求項 2 7】 前記ホストインタフェース制御回路は、前記利用情報ライセンスをホスト装置から受領して前記記憶媒体に格納可能であることを特徴とする請求項 2 6 記載のデータ処理装置。

【請求項 2 8】 前記ホストインタフェース制御回路は、前記コンテンツ鍵とともに入力される時間情報を前記アクセス時間情報の初期値として前記記憶媒体に格納可能であることを特徴とする請求項 2 7 記載のデータ処理装置。

【請求項 2 9】 ホストインタフェース部、媒体インタフェース部、及びデータ処理部を有し、媒体インタフェース部に装着された記憶媒体に所定の情報を格納するデータ処理装置であって、

前記データ処理部は、復号鍵の受領要求と共に記憶媒体が保有する証明情報をホストインタフェース部から外部に出力し、これに応答してホストインタフェース部に返される情報を受領し、これに基づいて、媒体インタフェース部から前記記憶媒体に、前記所定の情報として、利用情報を復号するための復号鍵と利用情報に対するアクセス制限を行なう制限情報とを格納し、

前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、

前記アクセス時間情報の初期値は前記受領した情報に含まれる時間情報であり

、
前記証明情報は特定の記憶媒体であることを表す情報であり、

前記特定の記憶媒体は、制御回路と不揮発性記憶回路とを有し、

前記不揮発性記憶回路は前記制限情報の格納領域を有し、

前記制御回路は、外部より供給される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行ない、

前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、

前記制御回路によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なうことを特徴とするデータ処理装置。

【請求項 3 0】 媒体インタフェース部、及びデータ処理部を有し、媒体インタフェース部に装着された記憶媒体に所定の情報を格納するデータ処理装置であって、

前記データ処理部は、復号鍵の発行要求に応答して記憶媒体から証明情報を取得し、記憶媒体を認証した後に、媒体インタフェース部から記憶媒体に、前記所定の情報として、利用情報を復号するための復号鍵と利用情報に対するアクセス制限を行なう制限情報とを格納し、

前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、

前記アクセス時間情報の初期値は所定に時間情報であり、

前記証明情報は特定の記憶媒体であることを表す情報であり、

前記特定の記憶媒体は、制御回路と不揮発性記憶回路とを有し、

前記不揮発性記憶回路は前記制限情報の格納領域を有し、

前記制御回路は、外部より供給される時刻情報と前記制限情報とに基いて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行ない、

前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定し、

前記制御回路によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なうことを特徴とするデータ処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、記憶媒体に格納された動画や音楽などのコンテンツデータなどに対する再生期限管理に係り、再生期限管理の制御を適用した不揮発性記憶装置、再生端末装置及び頒布端末装置に関する。

【0002】

【従来の技術】

メモ리카ードなどの記憶媒体に記憶された画像データおよび音楽データレンタルされる場合、予め設定された再生期限内であれば、ユーザは、再生装置を用いて画像および音楽を再生できる。ユーザの再生装置において検知された時刻と、記憶媒体にデジタルデータを記憶する時に書込まれた再生期限情報とに基づいて、再生が管理される。ユーザの再生装置により検知される現在時刻が改ざんされると、再生期限を経過しているにもかかわらず、コンテンツを再生することができる。

【0003】

再生装置の時刻改ざんに対する対策として、例えば特許文献1に記載された技術が有る。すなわち、データ書込み装置は、データ読取り装置によりデータを出力可能な期限を設定して、記憶媒体に、データと、期限と、記憶媒体へのデータおよび期限の書込み日時とを書込む。データ読取り装置は、記憶媒体から読取った期限と書込み日時と、検知した現在日時とに基づいて、記憶媒体に書込まれたデータの出力の可否を判断して、データの出力が可能であると、記憶媒体からデータを読取って出力する。データを出力できる期限が経過したときに、データ読

取り装置の検知手段により検知される現在日時を書込み日時以前に変更して、不正にデータの出力を行なおうとする場合を想定する。この場合、不正に変更された現在日時が、データが書込まれた日時以前であるため、判断手段は、データの出力が可能と判断しない。更に前記書き込み日時は再生処理の終了時に現在時刻に更新するようになっている。

【0 0 0 4】

【特許文献 1】

特開 2 0 0 2 - 2 5 9 9 1 7 号公報（段落 9 9、図 7）

【0 0 0 5】

【発明が解決しようとする課題】

上記特許文献 1 の技術によればメモリカード等の記憶媒体に日時データを記録することによって端末内部の時計を操作されても期限付きコンテンツの不正な再生を抑制することができるが、充分ではないことが本発明者によって見出された。第 1 に、記憶媒体の現在時刻を再生終了時点で更新するだけでは不十分な場合が想定される。例えばコンテンツ再生終了直前に電源が遮断された場合には記憶媒体の現在時刻が全く更新されない虞がある。第 2 に、期限付きコンテンツの不正再生抑制機能は再生装置側が備えるので、再生装置を変えれば依然として不正アクセスが可能になる。

【0 0 0 6】

本発明の目的は、再生装置や端末装置内部の時計の操作による期限付きデータの不正アクセスを効果的に抑制する技術を提供することにある。

【0 0 0 7】

本発明の前記並びにその他の目的と新規な特徴は本明細書の記述及び添付図面から明らかになるであろう。

【0 0 0 8】

【課題を解決するための手段】

本願において開示される発明のうち代表的なものの概要を簡単に説明すれば下記の通りである。

【0 0 0 9】

《不揮発性記憶装置》

本発明の第 1 の観点は、期限付きデータの不正アクセス抑止機能を記憶媒体としての不揮発性記憶装置が備える観点である。

【0 0 1 0】

〔1〕本発明に係る不揮発性記憶装置は、制御回路と不揮発性記憶回路とを有する。前記不揮発性記憶回路は利用情報に対するアクセス制限を行なう制限情報の格納領域を有する。前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれる。前記制御回路は、外部より供給される時刻情報と前記制限情報とに基づいて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行なう。前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定する。前記制御回路によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なう。

【0 0 1 1】

上記手段により、メモリカード等の不揮発性記憶装置にアクセス時間情報のような日時データを更新して記録するから、更新毎に、アクセス時間情報により示される時間と期限情報により示される時間差は狭められ、最後にアクセス時間情報により示される時間が期限情報により示される時間を超える。一端超えれば利用不可にされる。最早、ユーザーは端末内の時計を利用制限より前の日時に戻しても再生は不可とされる。これにより、再生装置などの端末内部の時計が操作されても期限付き利用情報の不正な再生を抑制することが可能になる。アクセス時間情報の更新はアクセス終了時点だけでなくアクセス開始時点でも行なわれるから、利用情報の再生終了直前に電源が遮断されても少なくとも 1 回のアクセス時間情報の更新は保証される。期限付き利用情報の不正再生抑制機能は不揮発性記憶装置が備えるので、再生装置を変えても依然として不正アクセス抑止機能を働かせることは容易である。

【0 0 1 2】

〔2〕アクセス判定動作は、少なくとも不揮発性記憶装置へ動作電源を投入するときと動作電源を遮断するときに行なうようにしてもよい。

【0013】

〔3〕更にアクセス判定動作を別のタイミングで行なってもよい。即ち、利用情報を複数に分割してアクセスを行なうとき、アクセス開始時の前記アクセス判定動作においてアクセス可と判定された後は、分割された前記利用情報のアクセス毎又は所定の複数アクセス毎に前記アクセス判定動作を行なってもよい。

【0014】

〔4〕分割された前記利用情報のアクセス単位は例えばセクタである。

【0015】

〔5〕前記分割された利用情報のアクセスに対するアクセス判定動作において、第2回目以降のアクセス判定動作では、時刻情報が前記アクセス期限情報により示されるアクセス期限より後であってもアクセス可と判定するようにしてよい。アクセス判定動作を何回も行なうとき、利用情報の再生途中などで期限が到来して再生が中断される不都合を簡単に解消することができる。

【0016】

〔6〕前記不揮発性記憶装置は、例えば前記時刻情報を出力可能な外部装置に接続され使用されるものであり、前記外部装置へ前記分割された利用情報を出力可能である。

【0017】

〔7〕前記不揮発性記憶回路は、例えば不揮発性半導体メモリであり、外部装置に接続されるインタフェース端子を有する所定のメモリカードケーシングに内蔵されて成る。

【0018】

〔8〕前記制限情報は前記制御回路により暗号化されて前記不揮発性記憶回路に格納される。アクセス制限が行なわれていない領域に格納される場合に、簡便で好適である。

【0019】

〔9〕前記制限情報の暗号化に用いる暗号鍵は、例えば不揮発性記憶装置固有

の属性情報にすればよい。

【 0 0 2 0 】

〔 1 0 〕 著作権保護の観点が考慮される場合には、前記制御回路は前記利用情報を復号するためのコンテンツ鍵を含む利用情報ライセンスを受領するために証明情報を外部に出力可能であることがよい。

【 0 0 2 1 】

〔 1 1 〕 その証明情報に対して外部で認証されれば、前記制御回路は、前記利用情報ライセンスを外部から受領することができ、受領したライセンスを前記不揮発性記憶回路に格納するのがよい。

【 0 0 2 2 】

〔 1 2 〕 前記制御回路は前記コンテンツ鍵とともに入力される時間情報を前記アクセス時間情報の初期値として前記不揮発性記憶回路に格納することが望ましい。そのような時間情報については改ざんされている可能性は非常に低い。

【 0 0 2 3 】

〔 1 3 〕 セキュア領域のようなアクセス制限領域について考慮する。前記不揮発性記憶回路はアクセス制限領域とアクセス非制限領域とを有するとき、前記制限情報はアクセス制限領域に格納し、前記利用情報はアクセス非制限領域に格納すればよい。

【 0 0 2 4 】

〔 1 4 〕 アクセス制限領域に対する書き込み認証について考慮する。前記制御回路は外部からの認証を受けて前記アクセス制限領域に対する書き込みが可能にされればよい。アクセス制限領域に対する不正な書き込みが阻止される。

【 0 0 2 5 】

〔 1 5 〕 前記アクセス制限領域は例えば前記利用情報ライセンス等の格納領域とされる。

【 0 0 2 6 】

〔 1 6 〕 アクセス制限領域に対する読み出し認証について考慮する。前記制御回路は外部から与えられる証明情報に対する認証を行なって前記アクセス制限領域に対する読み出しを可能にする。アクセス制限領域に対する不正な読み出しを

阻止できる。

【0027】

《再生端末装置》

本発明の第2の観点は、期限付きデータの不正アクセス抑止機能を再生端末などのデータ処理装置を備える観点である。

【0028】

〔17〕本発明に係るデータ処理装置は、再生部と利用制限部とを有し、利用情報に対するアクセス制限を行なう制限情報を書換え可能に格納する記憶媒体をアクセスして前記利用情報を再生可能である。前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれる。前記利用制限部は、データ処理装置で生成される時刻情報と前記制限情報とに基づいて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記記憶媒体上の前記アクセス時間情報を更新するアクセス判定動作を行なう。前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定する。前記利用制限部によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なう。

【0029】

上記手段により、メモリカード等の記憶媒体にアクセス時間情報のような日時データを更新して記録するから、更新毎に、アクセス時間情報により示される時間と期限情報により示される時間差は狭められ、最後にアクセス時間情報により示される時間が期限情報により示される時間を超える。一端超えれば利用不可にされる。最早、ユーザーは端末内の時計を利用制限より前の日時に戻しても再生は不可とされる。これにより、再生装置などの端末内部の時計が操作されても期限付きコンテンツの不正な再生を抑制することが可能になる。アクセス時間情報の更新はアクセス終了時点だけでなくアクセス開始時点でも行なわれるから、利用情報の再生終了直前に電源が遮断されても少なくとも1回のアクセス時間情報の更新は保証される。

【 0 0 3 0 】

〔 1 8 〕 アクセス判定動作は、少なくとも再生部へ記憶媒体を装着するときと再生部から記憶媒体を離脱するときに行なうようにしてもよい。

【 0 0 3 1 】

〔 1 9 〕 また別の大要としてアクセス判定動作は、再生部に記憶媒体が装着された状態で動作電源が投入されるときと、再生部に記憶媒体が装着された状態で動作電源が遮断されるときに行なうようにしてもよい。

【 0 0 3 2 】

〔 2 0 〕 前記利用制限部は、記憶媒体固有の属性情報を暗号鍵として暗号化を行なってアクセス時間情報の更新を行なう。アクセス制限が行なわれていない領域に格納される場合に、簡便で好適である。

【 0 0 3 3 】

〔 2 1 〕 前記記憶媒体は例えば書換え可能な不揮発性記憶装置である。

【 0 0 3 4 】

〔 2 2 〕 セキュア領域のようなアクセス制限領域について考慮する。前記不揮発性記憶装置はアクセス制限領域とアクセス非制限領域とを有するとき、前記利用制限判定部はアクセス制限領域に対して制限情報のアクセスを行ない、前記再生部はアクセス非制限領域に対して利用情報のアクセスを行なう。

【 0 0 3 5 】

〔 2 3 〕 アクセス制限領域に対する書き込み認証について考慮する。前記利用制限部は不揮発性記憶装置から出力される証明情報に対して認証を行なった後にアクセス制限領域に書き込みが可能にされるのがよい。アクセス制限領域に対する不正な書き込みが阻止される。

【 0 0 3 6 】

〔 2 4 〕 前記アクセス制限領域は前記利用情報を復号するための利用情報ライセンスの格納領域とされる。

【 0 0 3 7 】

〔 2 5 〕 アクセス制限領域に対する読み出し認証について考慮する。前記利用制限部は不揮発性記憶装置に証明情報を与えて認証を受けた後に前記アクセス制

限領域に対する読み出しが可能にされるのがよい。アクセス制限領域に対する不正読み出しを阻止できる。

【0038】

〔26〕ホストインタフェース制御部を有するとき、著作権保護の観点が考慮される場合には、当該ホストインタフェース制御部は、前記利用情報を復号するためのコンテンツ鍵を含む利用情報ライセンスを受領するために前記記憶媒体が保有する証明情報をホスト装置に向けて出力可能であることが望ましい。

【0039】

〔27〕その証明情報に対してホスト送致で認証されれば、前記ホストインタフェース制御回路は、前記利用情報ライセンスをホスト装置から受領して前記記憶媒体に格納可能であることが望ましい。

【0040】

〔28〕前記ホストインタフェース制御回路は、前記コンテンツ鍵とともに入力される時間情報を前記制アクセス時間情報の初期値として前記記憶媒体に格納可能であることが望ましい。そのような時間情報については改ざんされている可能性は非常に低い。

【0041】

《ダウンロード端末装置》

本発明の第3の観点は、期限付きデータの不正アクセス抑止機能をダウンロード端末装置等のデータ処理装置が支援する観点である。

【0042】

〔29〕本発明に係るデータ処理装置はホストインタフェース部、媒体インタフェース部、及びデータ処理部を有し、媒体インタフェース部に装着された記憶媒体に所定の情報を格納する。前記データ処理部は、復号鍵の受領要求と共に記憶媒体が保有する証明情報をホストインタフェース部から外部に出力し、これに応答してホストインタフェース部に返される情報を受領し、これに基づいて、媒体インタフェース部から前記記憶媒体に、前記所定の情報として、利用情報を復号するための復号鍵と利用情報に対するアクセス制限を行なう制限情報とを格納する。前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれる。前記

アクセス時間情報の初期値は前記受領した情報に含まれる時間情報である。前記証明情報は特定の記憶媒体であることを表す情報である。前記特定の記憶媒体は、制御回路と不揮発性記憶回路とを有し、前記不揮発性記憶回路は前記制限情報の格納領域を有する。前記制御回路は、外部より供給される時刻情報と前記制限情報とに基づいて前記利用情報のアクセス可否を判定し、前記時刻情報に基づいて前記アクセス時間情報を更新するアクセス判定動作を行なう。前記アクセス可否の判定において前記時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記時刻情報が前記アクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定する。前記制御回路によるアクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なう。

【0043】

《頒布端末装置》

本発明の第4の観点は、期限付きデータの不正アクセス抑止機能を頒布端末装置等のデータ処理装置が支援する観点である。

【0044】

〔30〕本発明に係るデータ処理装置は、媒体インタフェース部及びデータ処理部を有し、媒体インタフェース部に装着された記憶媒体に所定の情報を格納する。前記データ処理部は、復号鍵の発行要求に応答して記憶媒体から証明情報を取得し、記憶媒体を認証した後に、媒体インタフェース部から記憶媒体に、前記所定の情報として、利用情報を復号するための復号鍵と利用情報に対するアクセス制限を行なう制限情報とを格納する。前記制限情報にはアクセス期限情報とアクセス時間情報とが含まれ、前記アクセス時間情報の初期値は所定に時間情報である。前記証明情報は特定の記憶媒体であることを表す情報である。特定の記憶媒体は上記項目〔29〕の記憶媒体と同じである。

【0045】

【発明の実施の形態】

図1にはコンテンツデータ配信システムが例示される。コンテンツサーバ1が接続するネットワーク2には代表的に示される利用期限付きデータ端末装置（デ

ータ処理装置) 3が接続される。利用期限付きデータ端末装置(単にデータ端末装置とも称する) 3はダウンロード再生部(ダウンロード部及び再生部) 10、利用期限判定部(利用制限部) 11、及び端末内部時計 12を有する。データ端末装置 3には記憶媒体として不揮発性記憶装置(単にメモリカードとも称する) 13が着脱自在にされる。メモリカード 13はフラッシュメモリなどの電氣的に消去及び書き込み可能な不揮発性メモリ(不揮発性記憶回路) 14を備える。

【0046】

データ端末装置 3によるコンテンツデータのダウンロード機能の概略を説明する。データ端末装置 3にメモリカード 13が装着されて、データ端末装置 3にコンテンツデータのダウンロードが指示されると、データ端末装置 3は、コンテンツサーバ 1から利用期限付きコンテンツデータ(利用情報)とそれに対応した再生ライセンス(利用情報ライセンス)をダウンロードし、メモリカードに書き込む。更に、サーバ 1からダウンロードの日時データを取得し、メモリカード 13に書き込む。メモリカード 13に書き込まれた日時データがカード日時データである。特に制限されないが、ダウンロードされた日時データは利用制限判定部でライセンスフォーマットに組み込まれてセキュアライセンスとして不揮発性メモリ 14のセキュア領域に格納される。特に制限されないが、利用期限もセキュアライセンスが保有する。また、特に制限されないが、再生ライセンスも不揮発性メモリ 14のセキュア領域に格納される。

【0047】

データ端末装置 3による期限付きコンテンツデータの再生機能について概略を説明する。データ端末装置 3に再生が指示されるとデータ端末装置 3はメモリカード 13から再生ライセンスを読み出す。読み出した再生ライセンスから利用期限を取出し、コンテンツデータの利用期限を利用期限判定部 11に送る。利用期限部 11は、コンテンツデータの利用期限(アクセス期限情報)、端末内部時計 12が示す端末日時データ(時刻情報)、カードが保有するカード日時データ(アクセス時間情報)とによって、アクセス可否を判定する。即ち、前記端末日時データにより示される日時がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記端末日時データにより示される日時がカード日時データに

より示される日時よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定する。アクセス可であればメモリカード13のコンテンツデータを読み出して再生する。アクセス否であれば再生ライセンスなどを消去する。利用期限判定部11は前記アクセス可否判定と共に、前記端末日時データに基づいてメモリカード13内のカード日時データを更新する。

【0048】

カード日時データの更新は、上記アクセス可否判定時に代表されるアクセス開始時だけでなく、アクセス終了時にも行なう。また、例えば、少なくともメモリカードへ動作電源を投入するときと動作電源を遮断するときに行なうようにしてもよい。

【0049】

図2にはコンテンツデータ配信システムに別のデータ端末装置4が接続されている例が示される。データ端末装置4はダウンロード再生部（ダウンロード部及び再生部）10と端末内部時計12を有する。データ端末装置3には記憶媒体として不揮発性記憶装置（単にメモリカードとも称する）15が着脱自在にされる。メモリカード15は利用期限判定部（利用制限部）16と不揮発性メモリ14を備える。

【0050】

データ端末装置4によるコンテンツデータのダウンロード機能の概略を説明する。データ端末装置4にメモリカード15が装着されて、データ端末装置4にコンテンツデータのダウンロードが指示されると、データ端末装置4は、コンテンツサーバ1から利用期限付きコンテンツデータ（利用情報）とそれに対応した再生ライセンス（利用情報ライセンス）をダウンロードし、メモリカード15に書き込む。更に、サーバ1からダウンロードの日時データを取得し、メモリカード15に書き込む。メモリカード15に書き込まれた日時データがカード日時データである。特に制限されないが、ダウンロードされた日時データは利用制限判定部でライセンスフォーマットに組み込まれてセキュアライセンスとして不揮発性メモリ14のセキュア領域に格納される。特に制限されないが、再生ライセンスも不揮発性メモリ14のセキュア領域に格納される。

【0051】

期限付きコンテンツデータの再生機能について概略を説明する。データ端末装置 4 に再生が指示されるとデータ端末装置 4 は利用期限判定部 16 にメモリカード 15 の再生ライセンスを取得させる。利用期限判定部 16 は読み出した再生ライセンスから利用期限を取出す。利用期限判定部 16 は、コンテンツデータの利用期限（アクセス期限情報）、端末内部時計 12 が示す端末日時データ（時刻情報）、不揮発性メモリ 14 が保有するカード日時データ（アクセス時間情報）とによって、アクセス可否を判定する。即ち、前記端末日時データにより示される日時がアクセス期限情報により示されるアクセス期限よりも後であり、又は前記端末日時データにより示される日時がカード日時データにより示される日時よりも前である場合にアクセス否と判定し、その他の場合をアクセス可と判定する。アクセス可であれば利用期限判定部 16 はダウンロード再生部 10 にメモリカード 13 のコンテンツデータを読み出させて再生可能とする。利用期限判定部 16 は前記アクセス可否判定と共に、前記端末日時データに基づいてメモリカード内のカード日時データを更新する。

【0052】

カード日時データの更新は、上記アクセス可否判定時に代表されるアクセス開始時だけでなく、アクセス終了時にも行なう。また、例えば、少なくともメモリカードへ動作電源を投入するときと動作電源を遮断するときに行なうようにしてもよい。

【0053】

図 3 には前記端末日時データに基づいて更新されるカード日時データによる利用制限の概要が例示される。コンテンツデータをダウンロードした日時（借りた日） T_s 、利用期限（返却日） T_e は固定である。現在とある時間は端末日時データが示す時間 T_c である。アクセス日時とあるのがカード日時データが示す時間 T_{acs} である。カード日時データが更新されなければそれが示す日時はコンテンツデータをダウンロードした日時（借りた日） T_s に固定される。仮に（a）のように、カード日時データ T_{acs} が更新されなければ現在日時 T_c が借りた日 T_s と利用期限 T_e の間の何処にあっても利用可能となり、例えば（b）の

ように現在日時 T_c が利用期限 T_e を過ぎれば利用不可になる。しかし、端末時計を操作して現在日時を借りた日と利用期限の間に移動すれば、コンテンツデータは不正に利用可能になる。これに対し図 1、図 2 では前記端末日時データに基づいてメモリカード内のカード日時データを更新するから、(c) のようにアクセス日時とあるカード日時データ T_{acs} が示す日時から利用期限までの時間は更新毎に狭められ、最後に利用期限 T_e を超える。一端超えれば利用不可にされる。最早、ユーザーは端末内の時計を利用制限より前の日時に戻しても再生は不可とされる。これにより、データ端末装置内部の時計が操作されても期限付きコンテンツの不正な再生を十分に抑制することが可能になる。

【0054】

カード日時データの更新は、アクセス終了時点だけでなくアクセス開始時点でも行なわれるから、利用情報の再生終了直前に電源が遮断されても少なくとも 1 回のアクセス時間情報の更新は保証される。図 2 のように、期限付き利用情報の不正再生抑制機能は不揮発性記憶装置が備えるので、再生装置を変えても依然として不正アクセス抑止機能を働かせることは容易である。

【0055】

図 4 には前記利用期限判定部 11 と端末内部時計 12 の具体例が示される。20 で示される回路ブロックは、少なくとも前記利用期限判定部 11 と端末内部時計 12 を実現するマイクロコンピュータとされる。図 4 にはマイクロコンピュータ 20 の内部を機能ブロックによって示している。マイクロコンピュータ 20 は、日時データ取得作成部 21、暗号化部 22、ライセンス作成部 23、セキュア領域アクセス部 24、日時データ取り出し部 25、復号部 26、利用制限判定部 26、及び端末内時計回路 27 を有する。

【0056】

不揮発性メモリ 14 はセキュア領域（アクセス制限領域）14A と非セキュア領域（アクセス非制限領域）14B を有する。セキュア領域 14A に対する書き込みアクセスはメモリカード 13 内の証明情報に対しメモリカード外部例えば端末装置 20 やサーバ 1 による認証を受けて可能にされる。外部からセキュア領域 14A に対する読み出しは外部から与えられる証明情報に対して認証を得ること

を条件に許可される。図示は省略するが、メモリカード 13 は不揮発性メモリ 14 のアクセス制御と外部とのインタフェース制御を行なうカードコントローラを有している。セキュア領域アクセス部 24 はそのカードコントローラを介してインタフェースされる。

【0057】

この例では、カード日時データ暗号化部 22 で暗号化した後、これをライセンス作成部 23 でセキュアライセンスに埋め込んで、セキュア領域アクセス部 24 の制御で不揮発性メモリ 14 のセキュア領域 14A に記録するようになっている。

【0058】

前記日時データ取得作成部 21 はサーバ 1 がコンテンツデータやライセンスをダウンロードしたときサーバ 1 から日時データ（ダウンロード日時データ）を取得する回路である。取得した日時データのフォーマットは図 5 に例示されるように、16 バイトのデータで構成される。

【0059】

前記暗号化部 22 はサーバから取得した前記日時データを暗号化する。暗号化方式は、特に制限されないが、コンテンツの暗号化復号処理で用いているのと同じ AES（Advanced Encryption Standard）方式を用いる。日時データを暗号化する鍵はメモリカード固有の属性情報、例えば、カードのシリアル番号等を用いる。

【0060】

前記ライセンス作成部 23 は、取得して暗号化した日時データを例えばライセンスフォーマット中のコンテンツ鍵の部分に埋め込んでセキュアライセンスを作成する。

【0061】

前記セキュア領域アクセス部 24 は日時データが含まれているセキュアライセンスを不揮発性メモリのセキュア領域 14A に書き込む。セキュア領域 14A への書き込みには前記書き込み認証が必要とされる。前記日時データ取り出し部 25 は暗号化された日時データが含まれるライセンスをセキュア領域から読み出し

、暗号化された日時データを取出す。セキュア領域 14A の読み出しには前記読み出し認証が必要とされる。

【0062】

復号部 26 はセキュアライセンスから取出した暗号化された日時データを AES で復号する。復号する鍵は暗号部 22 で用いた鍵と同じものを使用する。

【0063】

前記利用制限判定部 27 は、前述の如く、利用期限が切れていないのかを判定すると共に、端末内の時計がユーザーによって操作されていないかを判定する。その判定内容は図 1 を参照して既に説明した。操作されていると判定したら、カード内のライセンスを全て消去する。端末内時計回路 28 は端末内の時計から年月日時間を取得する。

【0064】

図 4 の各機能ブロックは、特に図示はしないが、中央処理装置、浮動小数点演算ユニット、それらの処理プログラムを保有する ROM（リード・オンリ・メモリ）、中央処理装置のワーク領域などに利用される RAM（ランダム・アクセス・メモリ）、リアルタイムクロック回路、タイマ、及び入出力回路などによって構成される。

【0065】

図 4 の回路の動作を説明する。最初に、サーバ 1 と通信したときやコンテンツ、ライセンスをダウンロードしたときの動作を説明する。

【0066】

サーバ 1 と接続したとき、サーバ 1 から日時データを日時データ取得・作成部 21 で取得する。取得した日時データはライセンスフォーマット中のコンテンツ鍵の領域に組込み可能にするために、日時データは例えば図 5 に例示する 16 バイトのデータ構成とされる。日時が 2002 年 10 月 10 日（木）15 時 30 分 45 秒 00 のとき、この日時データを 16 進で表すと、“07D2 000A 000A 0004 000F 001E 002D 0000 h” となる。

【0067】

暗号化部 22 で、日時データ取得・作成部 21 で作成した 16 バイトの日時デ

ータを A E S 方式で暗号する。暗号化する鍵はカード固有のシリアル番号を使用する。

【0 0 6 8】

ライセンス作成部 2 3 で、暗号化した日時データをライセンス内のコンテンツ鍵の部分に埋め込み、1 つのライセンスを作成する。作成されたライセンスは、セキュア領域アクセス部 2 4 によってメモリカードのセキュア領域に書き込まれる。セキュア領域が 1 2 8 個のライセンスを記録できる場合には、最後の 1 2 8 番目に日時データを含むライセンスを書き込む。セキュア領域 1 4 A に対する書き込みは前記書き込み認証を受けて可能にされる。

【0 0 6 9】

次に利用制限判定処理の動作について説明する。セキュア領域アクセス部 2 4 で、セキュア領域 1 4 A から暗号化されている日時データが含まれているセキュアライセンスを読み出す。セキュア領域に対するリードアクセスは前記読み出し認証を受けて可能にされる。日時データ取出し部 2 5 で、読み出したライセンスから暗号化されている日時データ 1 6 バイトを取出す。復号化部 2 6 で、1 6 バイトの日時データを A E S 方式で復号する。復号化する鍵は暗号化したときと同じカード固有のシリアル番号を使用する。次いで、端末内時計取得部 2 8 で、端末内の日時を取得する。利用制限判定部 2 7 で、利用期限、端末の日時データ、カードの日時データを用いて期限が切れていないのか、不正な操作が行われていないのかを判定する。

【0 0 7 0】

次に日時データの更新処理動作について説明する。カード内には電源がないため、カード自身では日時データを更新することはできない。したがって、上記で説明したようにサーバーとの接続時やコンテンツの再生、表示時（利用制限判定処理のとき）に日時データを更新する。しかし、サーバーと接続をしない場合やコンテンツの再生表示を行わない場合には長時間更新されない場合がある。日時データを更新するタイミングは、前述のアクセス開始時と終了時の他に、メモリカードがデータ端末に挿入されたときと離脱されたとき、或はメモリカードがデータ端末に装着されている状態でデータ端末の電源オンが指示されたときと、電

源オフが指示されたとき等であってよい。データ端末の電源をオフにするときには、マイクロコンピュータ内部のタイマーで測定した時間をカードに記録されている日時データに加算することにより更新すればよい。

【0071】

図6には前記メモリカード15に内蔵された前記利用期限判定部16の具体例が示される。前記利用期限判定部16はマイクロコンピュータ30によって構成される。図6ではマイクロコンピュータ30は外部インタフェースコントローラ31及びメモリコントローラ32と共にカードコントローラを構成する。図6にはマイクロコンピュータ30をその一部の機能である利用期限判定部16を構成する機能ブロックによって図示している。マイクロコンピュータ30によって実現される図示された機能ブロックは、暗号化部33、ライセンス作成部34、日時データ取り出し部35、復号部36、利用期限取り出し部37、及び利用制限判定部38である。

【0072】

外部インタフェースコントローラ31はマイクロコンピュータ30の指示に従って所定のメモリカードインタフェース仕様に準拠した外部インタフェース制御を行なう。メモリコントローラ32はマイクロコンピュータ30の指示に従って不揮発性メモリ14に対する消去、書き込み及び読み出しのアクセス制御を行なう。

【0073】

特に図示はしないが、マイクロコンピュータ30は中央処理装置、浮動小数点演算ユニット、それらの処理プログラムを保有するROM（リード・オンリ・メモリ）、中央処理装置のワーク領域などに利用されるRAM（ランダム・アクセス・メモリ）、リアルタイムクロック回路、タイマ、及び入出力回路などによって構成される。マイクロコンピュータ30は前記利用期限判定部16を実現すると共に、その動作プログラムに従って認証のための演算処理や不揮発性メモリ14をアクセスするためのアドレス演算処理等を行なう機能を有する。

【0074】

不揮発性メモリ14はセキュア領域（アクセス制限領域）14Aと非セキュア

領域（アクセス非制限領域）14Bを有する。セキュア領域14Aに対する書き込みアクセスはメモリカード15内の証明情報に対しメモリカード外部例えば端末装置20やサーバ1による認証を受けて可能にされる。外部からセキュア領域14Aに対する読み出しは外部から与えられる証明情報に対して認証を得ることを条件に許可される。メモリカード15内の前記証明情報は、そのメモリカード15が図2及び図6で説明した利用期限判定機能などを備えたメモリカードであり、その他のメモリカードと区別可能な情報を含んでいる。

【0075】

この例では、カード日時データ暗号化部33で暗号化した後、これをライセンス作成部34でセキュアライセンスに埋め込み、メモリコントローラ32を介して不揮発性メモリ14のセキュア領域14Aに記録するようになっている。特に制限されないが、コンテンツの利用期限もセキュアライセンスが保有する。

【0076】

図2のダウンロード再生部10がコンテンツデータやライセンスをサーバからダウンロードしたときサーバ1から日時データ（ダウンロード日時データ）が取得される。日時データはコンテンツライセンスに付随する。取得した日時データのフォーマットは図5に例示されるように、16バイトのデータで構成される。

【0077】

前記暗号化部33はサーバから取得した前記日時データを受取って暗号化する。暗号化方式は、特に制限されないが、コンテンツの暗号化復号処理で用いているのと同じAES（Advanced Encryption Standard）方式を用いる。日時データを暗号化する鍵はメモリカード固有の属性情報、例えば、カードのシリアル番号等を用いる。

【0078】

前記ライセンス作成部34は、取得して暗号化した日時データを例えばライセンスフォーマット中のコンテンツ鍵の部分に埋め込んでセキュアライセンスを作成する。

【0079】

作成されたセキュアライセンスはメモリコントローラ32を介して不揮発性メ

モリのセキュア領域 14 A に書き込まれる。セキュア領域 14 A への書き込みには前記書き込み認証が必要とされる。前記日時データ取り出し部 36 は暗号化された日時データが含まれるセキュアライセンスがセキュア領域 14 A から読み出されたとき、そこから暗号化された日時データを抽出する。利用期限取り出し部 37 はセキュアライセンスがセキュア領域 14 A から読み出されたとき、そこから利用期限データを抽出する。セキュア領域 14 A の読み出しには前記読み出し認証が必要とされる。

【0080】

復号部 36 はセキュアライセンスから取出した暗号化された日時データを AES で復号する。復号する鍵は暗号部 33 で用いた鍵と同じものを使用する。

【0081】

前記利用制限判定部 27 は、前述の如く、利用期限が切れていないのかを判定すると共に、データ端末 4 内の時計 12 がユーザーによって操作されていないかを判定する。その判定内容は図 2 を参照して既に説明した。操作されていると判定したら、セキュア領域 14 A 内のライセンスを全て消去する。

【0082】

図 6 の回路の動作を説明する。最初に、サーバ 1 と通信したときやコンテンツ、ライセンスをダウンロードしたときの動作を説明する。

【0083】

データ端末装置 4 がサーバ 1 に接続したとき、サーバ 1 からの日時データを外部インタフェースコントローラ 31 を介して入力する。併せて再生期限日データも入力する。再生期限日は例えば再生ライセンスに含まれるものを利用する。入力した日時データは図 5 に例示する 16 バイトのデータ構成とされる。日時データは暗号化部 33 によって例えば AES 方式で暗号される。暗号化する鍵はカード固有のシリアル番号を使用する。

【0084】

ライセンス作成部 34 で、暗号化した日時データをライセンス内のコンテンツ鍵の部分に埋め込み、セキュアライセンスを作成する。作成されたライセンスは、メモリコントローラ 32 を介してメモリカード 14 のセキュア領域 14 A に書

き込まれる。セキュア領域が 1 2 8 個のライセンスを記録できる場合には、最後の 1 2 8 番目に前記セキュアライセンスを書き込む。セキュア領域 1 4 A に対する書き込みは前記書き込み認証を受けて可能にされる。

【0 0 8 5】

次に利用制限判定処理の動作について説明する。メモリコントローラ 3 2 を介してセキュア領域 1 4 A からセキュアライセンスが読み出される。セキュア領域に対するリードアクセスは前記読み出し認証を受けて可能にされる。日時データ取出し部 3 5 で、読み出したライセンスから暗号化されている日時データ 1 6 バイトを取出す。利用期限取り出し部 3 7 では利用期限を取出す。復号部 3 6 で、1 6 バイトの日時データを A E S 方式で復号する。復号する鍵は暗号化したときと同じカード固有のシリアル番号を使用する。次いで、端末内の日時を取得する。利用制限判定部 3 8 で、利用期限、端末の日時データ、カードの日時データを用いて期限が切れていないのか、不正な操作が行われていないのかを判定する。

【0 0 8 6】

次に日時データの更新処理動作について説明する。カード内には電源がないため、カード自身では日時データを更新することはできない。したがって、上記で説明したようにサーバーとの接続時やコンテンツの再生、表示時（利用制限判定処理のとき）に日時データを更新する。しかし、サーバーと接続をしない場合やコンテンツの再生表示を行わない場合には長時間更新されない場合がある。日時データを更新するタイミングは、前述のアクセス開始時と終了時の他に、メモリカードがデータ端末に挿入されたときと離脱されたとき、或はメモリカードがデータ端末に装着されている状態でデータ端末の電源オンが指示されたときと、電源オフが指示されたとき等であってよい。データ端末の電源をオフにするときには、マイクロコンピュータ内部のタイマーで測定した時間をカードに記録されている日時データに加算することにより更新すればよい。

【0 0 8 7】

更新処理を、更に別のタイミングで行なってもよい。即ち、メモリカードがファイルメモリ方式によるセクタ単位で分割してデータアクセスを行なう場合、アクセス開始時の前記アクセス判定動作においてアクセス可と判定された後は、後

続セクタのアクセス毎又は所定の複数アクセス毎に前記アクセス判定動作を行なってもよい。このようにセクタ単位で分割されたデータのアクセスに対するアクセス判定動作において、第2回目以降のアクセス判定動作では、時刻情報が前記アクセス期限情報により示されるアクセス期限より後であってもアクセス可と判定するようにしてよい。アクセス判定動作を何回も行なうとき、利用情報の再生途中などで期限が到来して再生が中断される不都合を簡単に解消することができる。

【0088】

図7には再生ライセンスのフォーマットが例示され、図8にはセキュアライセンスのフォーマットが例示される。コンテンツIDはコンテンツ毎にユニークに割り当てられる識別子である。トランザクションIDはトランザクション毎にユニークな識別子である。トランザクションIDには再生可能回数（ライセンスを読み出せる回数）、移動可能回数（ライセンスを移動できる回数）、及びセーフレベル（保護強度）の識別子を含む。メディアアクセス条件はメディア内部で強制可能なアクセス条件である。コンテンツ鍵はコンテンツを暗号化するときに用いた鍵であり、コンテンツを復号する時に利用する。デコーダアクセス条件は再生用デコーダの内部で強制可能なアクセス条件を示す。デコーダアクセス条件には再生サイズ（1つのライセンスで再生可能なコンテンツサイズ）と利用期限（利用可能な期限）とを含む。拡張メディアアクセス条件は証明書認証、PIN認証を行うか否かを示すフラグとされる。再生ライセンスはコンテンツ鍵を有しているが、セキュアライセンスは、その再生ライセンスのコンテンツ鍵をカード日時データに入れ替えて構成される。

【0089】

証明書認証例えばセキュア領域の書き込み認証を受けるための証明情報、そしてPIN（Personal Identification Number）による個人認証を行なうためのPINは不揮発性メモリ14に格納されている。

【0090】

図9にはライセンスの書き込み時の認証（書き込み認証）処理手順が例示される。まず、証明認証を行なうか否かが判定され（S1）、行なう場合にはメモリ

カードから認証情報と公開暗号鍵を有する証明書（メディアクラス証明書）を読み出し（S2）、これをサーバに送信する（S3）。サーバはその証明書を検証し（S4）、それによって認証されれば、メモリカードのセキュア領域に対する再生ライセンス及びセキュアライセンスの書き込みが許容される（S5）。前記メディアクラス証明書は、例えば前記利用期限判定機能などを備えたメモリカード15を、当該機能を備えていない他のメモリカードと区別することができる証明情報を有している。

【0091】

図10にはライセンスの読み出し時の認証（読み出し認証）処理手順が例示される。まず、証明認証を行なうか否かが判定され（S11）、行なう場合にはデータ端末からメモリカードに認証情報と公開暗号鍵を有する証明書（デコードクラス証明書）を送信する（S12）。メモリカードはその証明書を検証し（S3）、それによって認証されれば、メモリカードのセキュア領域から再生ライセンス及びセキュアライセンスの読み出しが許容される（S14）。処理S11の判別で証明認証を行なわない場合には、PIN認証を行なうかの判別を行ない（S15）、行なう場合にはデータ端末装置からPINをメモリカードに送信し（S16）、メモリカード内でPINの検証を行なう。PINが正当であればライセンスの読み出しを行なう（S14）。PINが不当である場合、PIN認証を行なわない場合、証明認証を得られない場合にはそのまま処理を終了する。

【0092】

図11には利用期限付コンテンツの再生処理フローの一例が示される。再生ライセンスを利用して利用期限付コンテンツの再生を行なう場合、まず利用期限判定処理R21を行ない、再生可能であればカード日時データ更新処理R22を行ない、利用期限付コンテンツの再生終了を判定し（S23）、終了でなければ所定のインターバル毎にカード日時データ更新処理R22を繰り返す。再生終了を判別すると、最後にカード日時更新処理R22を行なって終了する。

【0093】

図12には利用期限判定処理R21の詳細な一例が示される。データ端末装置の日時情報を取得し、端末日時データを作成する（S31）。次に、必要な証明

認証又は P I N 認証を行なってメモリカードから、カード日時データを取得し (S 3 2)、ライセンスから利用期限を取得する (S 3 3)。利用制限とカード日時データを比較し (S 3 4)、利用期限 \leq カード日時データの場合には期限切れと判定して処理を終了する。利用期限 $>$ カード日時データの場合には端末日時データとカード日時データを比較する (S 3 5)。端末日時データ \leq カード日時データの場合には端末日時データが不正と判定し、メモリカードが保有する全てのライセンスの消去を行なう (S 3 6)。端末日時データ $>$ カード日時データの場合にはカードの日時データを端末の日時データに更新する (S 3 7)。

【0094】

図 1 3 にはカード日時データ更新処理 R 2 2 の詳細な一例が示される。データ端末装置の日時情報を取得し、端末日時データを作成する (S 4 1)。次に、必要な証明認証又は P I N 認証を行なってメモリカードから、カード日時データを取得する (S 4 2)。端末日時データとカード日時データを比較する (S 4 3)。端末日時データ \leq カード日時データの場合には端末日時データが不正と判定し、メモリカードが保有する全てのライセンスの消去を行なう (S 4 4)。端末日時データ $>$ カード日時データの場合にはカードの日時データを端末の日時データに更新する (S 4 5)。図 1 3 の処理は図 1 2 に対して、ライセンスから利用期限を取得せず、利用期限 \leq カード日時データの場合に期限切れと判定して処理を終了することを行なわない。したがって、利用期限付コンテンツの再生途中などで再生期限が到来して再生が中断される不都合を解消することができる。

【0095】

図 1 4 には期限付きデータの再生端末装置 4 0 が示される。同図に示される再生端末装置 4 0 は再生部 4 1 を有し、図 2 の端末装置 4 に対しコンテンツデータとライセンスのダウンロード機能が省かれた再生専用器として構成される。図 1 1 乃至図 1 3 に示されるコンテンツ再生処理を行なうことができる。

【0096】

図 1 5 にはダウンロード端末装置 4 5 が示される。同図に示されるダウンロード端末装置 4 5 は図 2 で説明した端末装置 4 におけるダウンロード再生部 1 0 に対しコンテンツデータの再生機能が省かれた、コンテンツデータとライセンスの

ダウンロード専用端末装置とされる。ダウンロード専用端末装置 45 は、ホストインタフェース部 46、メモリカードインタフェース部 47、及びデータ処理部 48 を有し、メモリカードインタフェース部 47 に装着されたメモリカード 15 に、コンテンツを復号するためのコンテンツライセンス、コンテンツに対するアクセス制限を行なう再生期限データ、及びカード日時データを初期的に格納する。前記データ処理部 48 は、前記コンテンツライセンスの受領要求と共にメモリカード 15 が保有する証明情報をホストインタフェース部 46 から外部に出力し、これに応答して例えばサーバ 1 からホストインタフェース部 46 に返される情報を受領してメモリカードインタフェース部 47 から前記メモリカード 15 に格納する。前記受領する情報は、コンテンツの復号に利用されるコンテンツ鍵、コンテンツに対するアクセス制限を行なう再生期限データ、及びカード日時データを含む。前記証明情報は利用期限判定機能を有するメモリカード 15 であることを表す情報である。このダウンロード端末装置を用いてメモリカードにコンテンツ及びその再生ライセンスを頒布もしくは販売することにより、対象となる記憶媒体が前記利用期限判定機能を有するメモリカード 15 に限定されるから、期限付きコンテンツデータに対する不正アクセスの抑止を支援することができる。

【0097】

図 15 の構成はネットワークに接続する端末装置としての構成に限定されない。特に図示はしないが、ダウンロード端末装置 45 それ自体がコンテンツサーバであってもよく、見方を変えればスタンドアロンの頒布端末装置となる。

【0098】

以上本発明者によってなされた発明を実施形態に基づいて具体的に説明したが、本発明はそれに限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは言うまでもない。

【0099】

例えば、今まで説明したダウンロード機能を有するデータ端末はコンテンツ及びコンテンツライセンスの双方をダウンロードして頒布する機能を有するものとして説明したが、本発明はそれに限定されず、コンテンツライセンスだけのダウンロード若しくは頒布であってもよい。また、再生機能を有するデータ端末装置

において、コンテンツはライセンスと同じメモリカードに格納されていなくてもよい場合がある。その場合、コンテンツデータはCD-ROMやDVD-RAM等のリムーバブルディスクドライブを用いてアクセスするようにしてもよい。或はハードディスクドライブからアクセスするようにしてもよい。

【0100】

また、上記説明では、日時データを暗号化してライセンスに埋め込んでセキュア領域に記録する例を示したが、暗号化を省いても良い。日時データを暗号化しないでライセンスに埋め込むため処理量が少なくて済む。また、日時データを暗号化して非セキュア領域に記録してもよい。セキュア領域を持たない記憶媒体にも使用できる。また、日時データを暗号化せず且つ非セキュア領域に記録してもよい。セキュア領域を持たない記憶媒体にも使用でき、しかも、AESの暗号／復号処理をする必要がないため最小の構成で実現できる。しかし、ユーザーにより日時データを操作される可能性が大きいことに注意を要する。

【0101】

【発明の効果】

本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば下記の通りである。

【0102】

すなわち、メモリカード等の不揮発性記憶装置にアクセス時間情報のような日時データを更新して記録し、しかもアクセス時間情報の更新はアクセス終了時点だけでなく複数時点で行なうから、利用情報の再生終了直前に電源が遮断されても少なくとも1回のアクセス時間情報の更新は保証される。期限付き利用情報の不正再生抑制機能を不揮発性記憶装置が備えることにより、再生装置を変えても依然として不正アクセス抑止機能を働かせることが容易である。

【図面の簡単な説明】

【図1】

本発明を適用したコンテンツデータ配信システムのブロック図である。

【図2】

本発明を適用したコンテンツデータ配信システムに別のデータ端末装置が接続

されている例を示す説明図である。

【図 3】

端末日時データに基づいて更新されるカード日時データによる利用制限の概要を例示する説明図である。

【図 4】

図 1 における利用期限判定部と端末内部時計の具体例を示すブロック図である。

【図 5】

日時データのフォーマットを例示する説明図である。

【図 6】

図 2 のメモリカードに内蔵された利用期限判定部の具体例を示すブロック図である。

【図 7】

再生ライセンスのフォーマットを例示する説明図である。

【図 8】

セキュアライセンスのフォーマットを例示する説明図である。

【図 9】

ライセンスの書き込み時の認証（書き込み認証）処理手順を例示するフローチャートである。

【図 1 0】

ライセンスの読み出し時の認証（読み出し認証）処理手順を例示するフローチャートである。

【図 1 1】

利用期限付コンテンツの再生処理の一例を示すフローチャートである。

【図 1 2】

図 1 1 の利用期限判定処理 R 2 1 の詳細を例示するフローチャートである。

【図 1 3】

図 1 1 のカード日時データ更新処理 R 2 2 の詳細を例示するフローチャートである。

【図 14】

期限付きデータの再生端末装置を例示するブロック図である。

【図 15】

ダウンロード端末装置を例示するブロック図である。

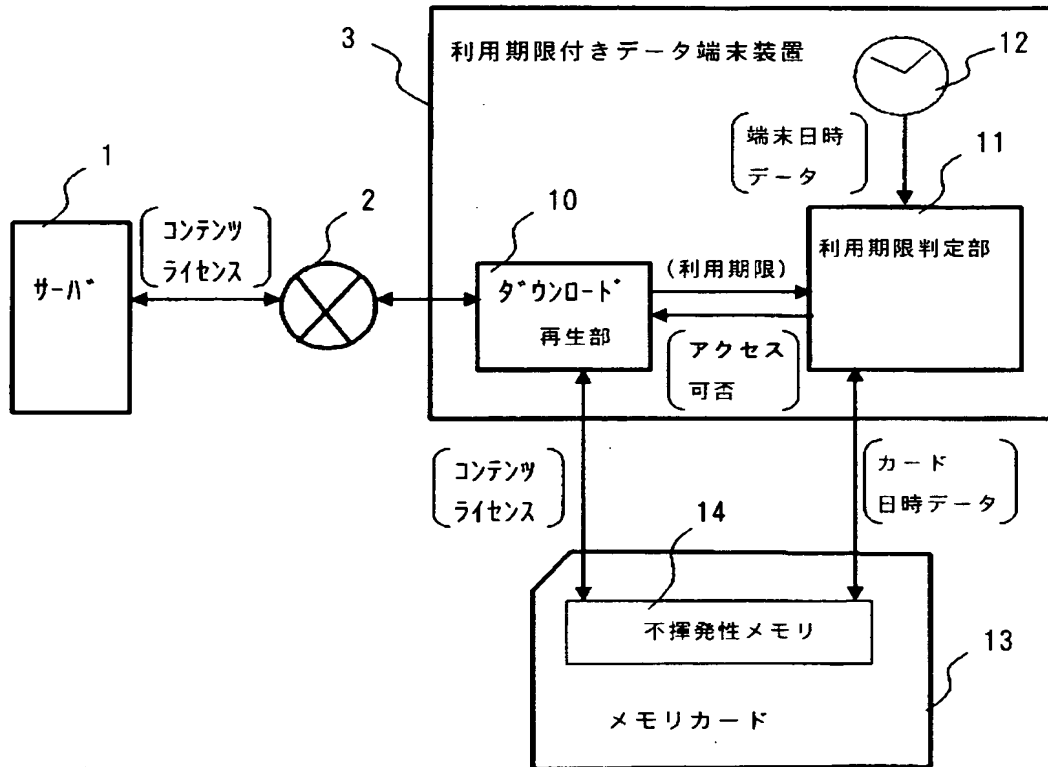
【符号の説明】

- 1 サーバ
- 2 ネットワーク
- 3 データ端末装置
- 4 データ端末装置
- 10 ダウンロード生成部
- 11 利用期限判定部
- 12 端末内部時計
- 13 メモリカード
- 14 不揮発性メモリ
- 14A セキュア領域（アクセス制限領域）
- 14B 非セキュア領域（アクセス非制限領域）
- 15 メモリカード
- 16 利用期限判定部
- 20 マイクロコンピュータ
- 30 マイクロコンピュータ
- 40 再生端末装置
- 41 再生部
- 45 ダウンロード専用端末装置
- 46 ホストインタフェース部
- 47 メモリカードインタフェース部
- 48 データ処理部

【書類名】 図面

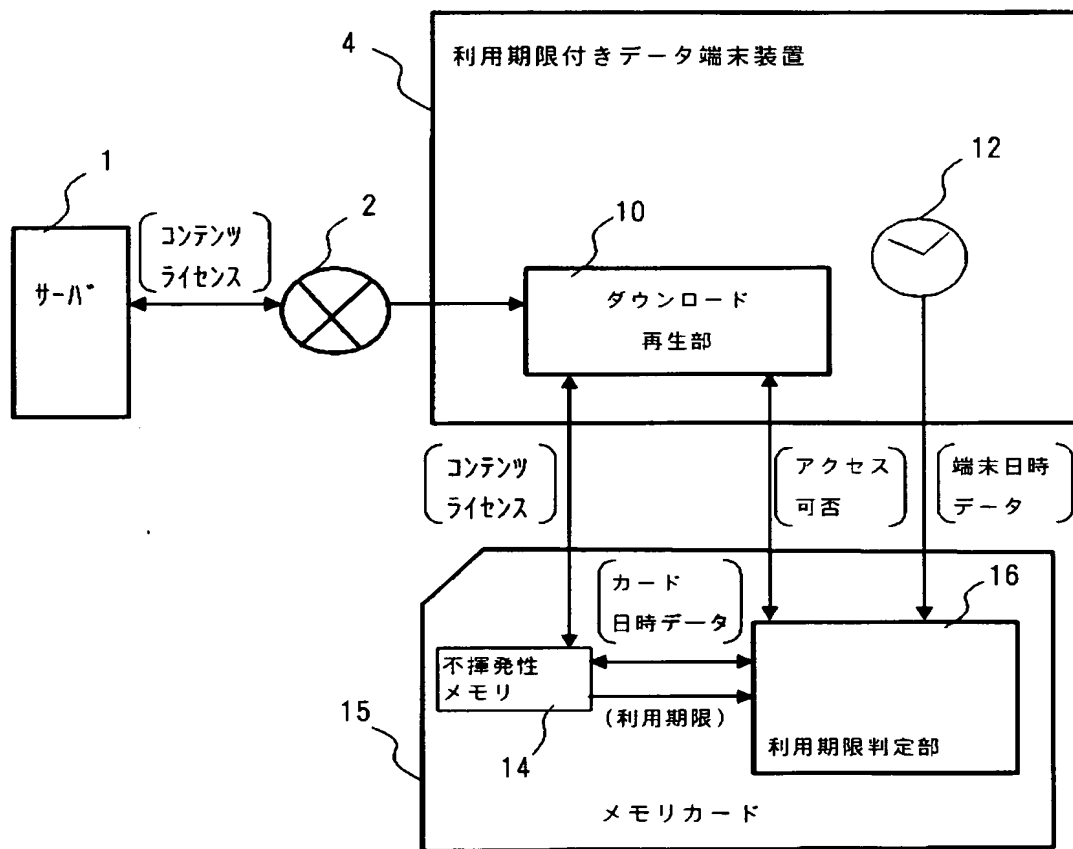
【図 1】

図 1



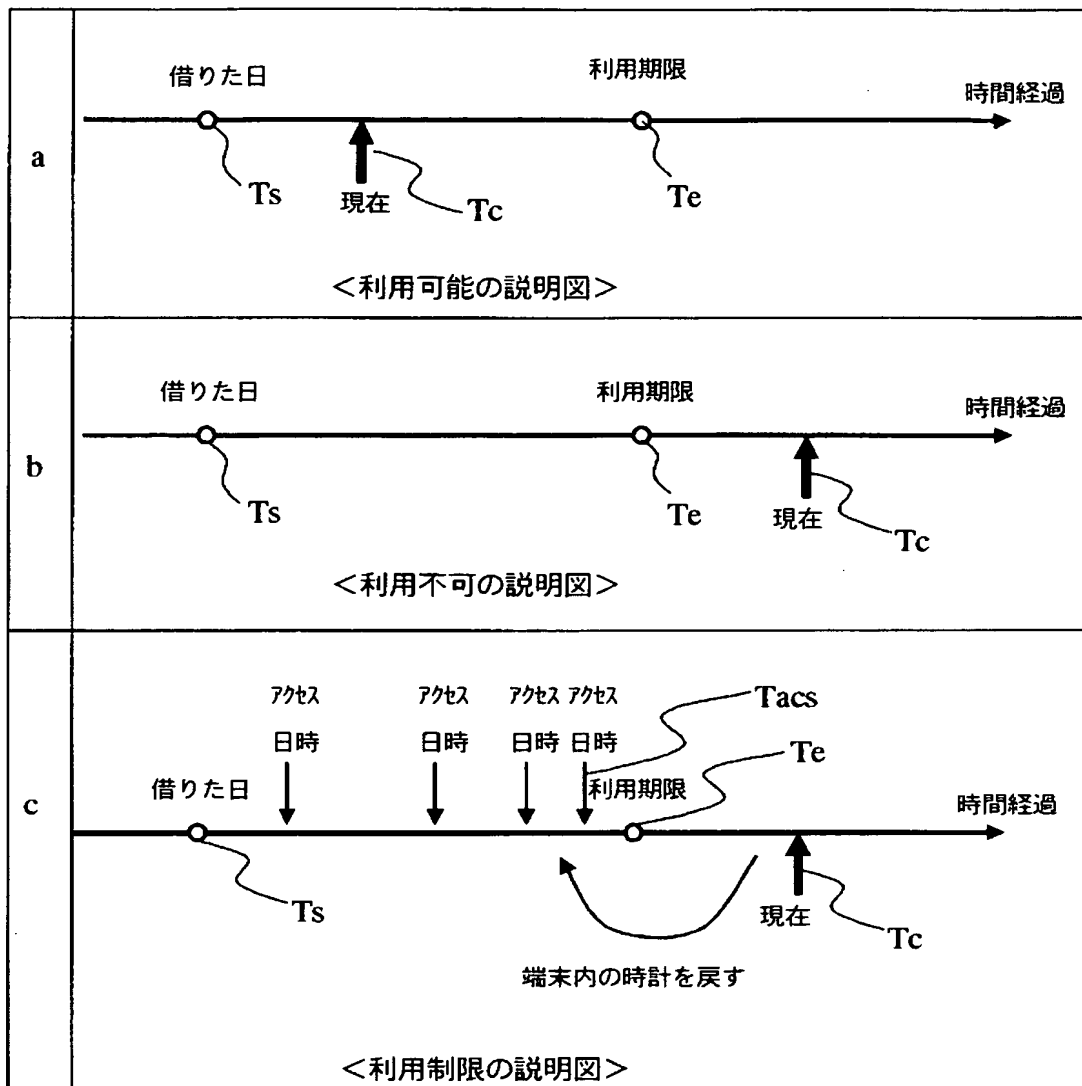
【図 2】

図 2

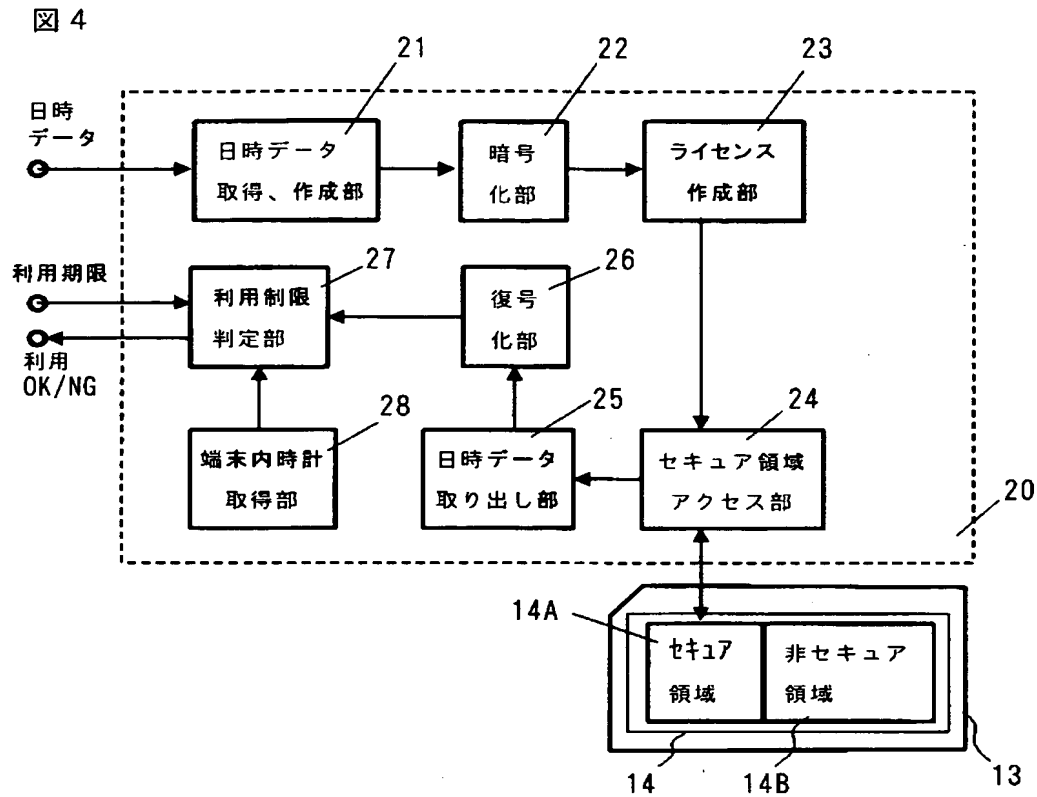


【図 3】

図 3

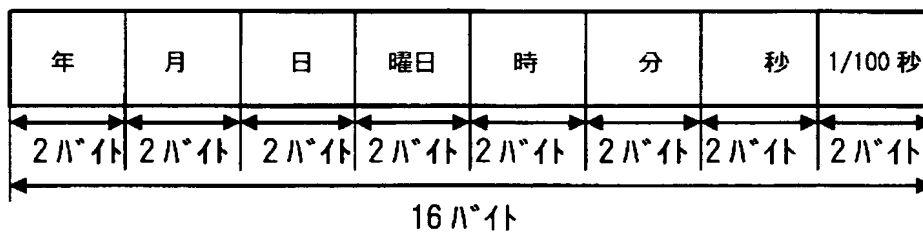


【図 4】



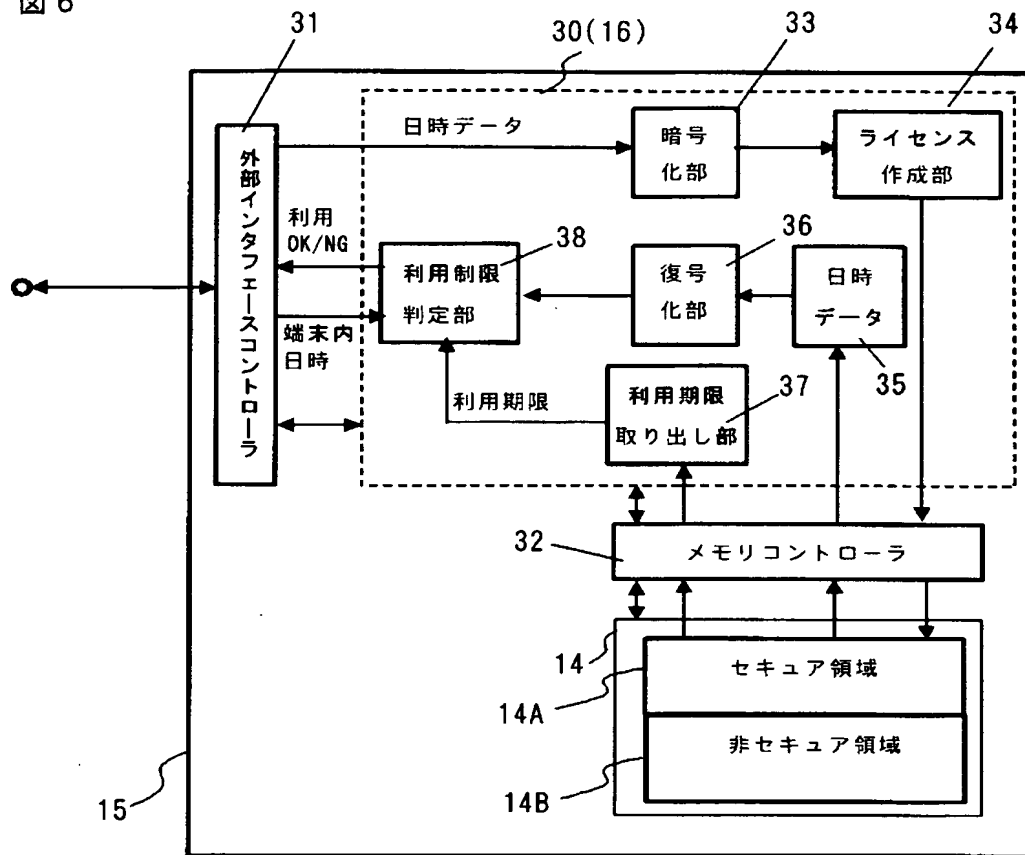
【図 5】

図 5



【図 6】

図 6



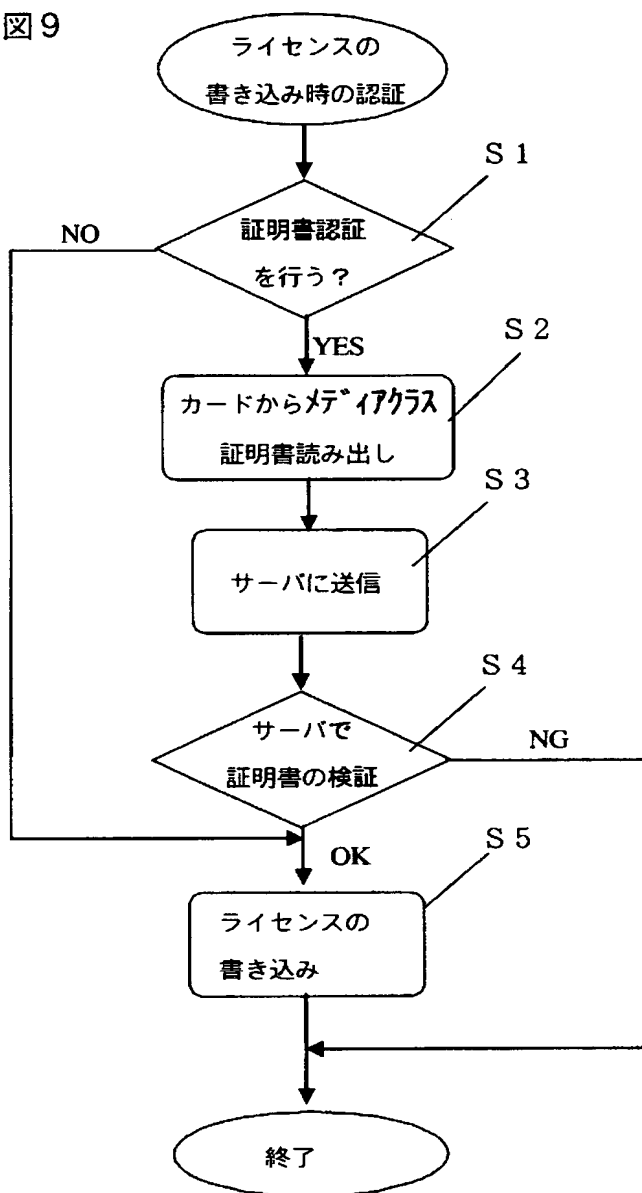
【図 7】

図 7

コンテンツ ID	トランザクション ID	メディア アクセス条件	コンテンツ 鍵	デコーダ アクセス条件	拡張メディア アクセス条件
		再生可能回数	移動可能回数	セーフレベル	再生サイズ
					利用期限

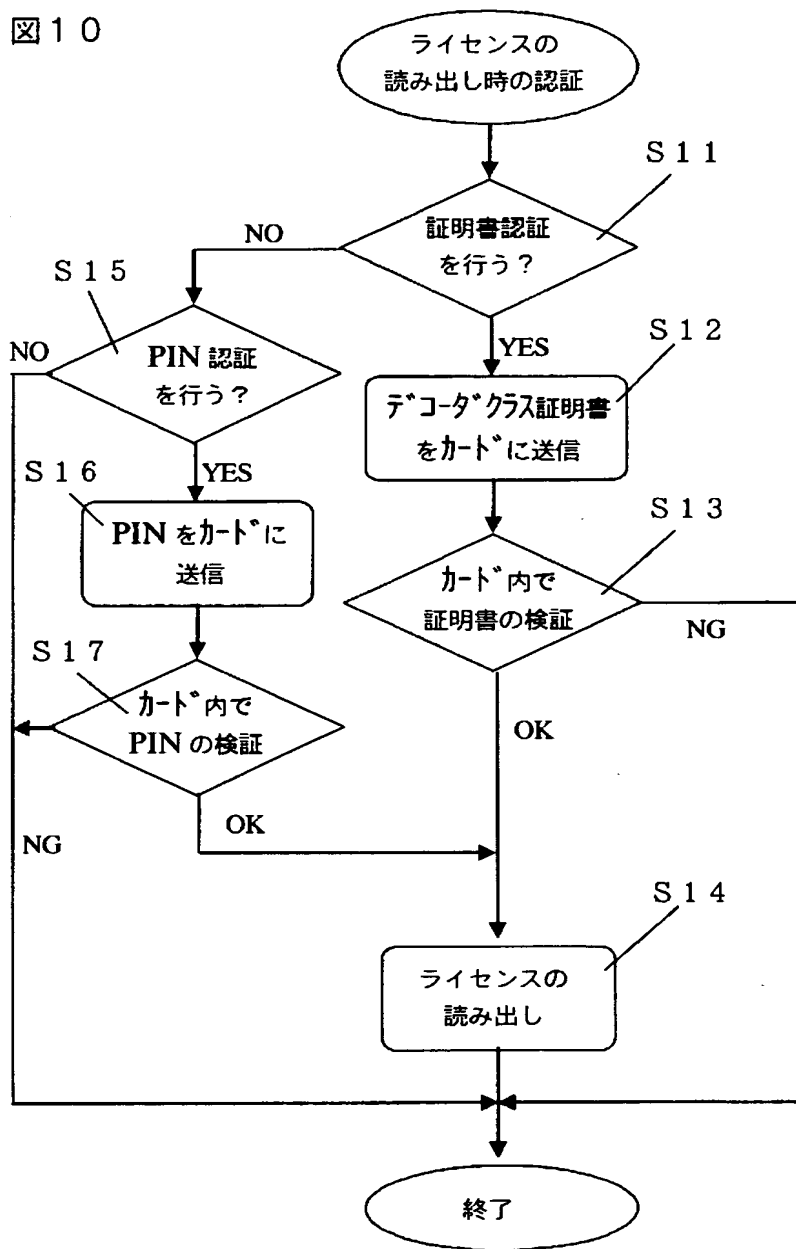
【図 9】

図 9



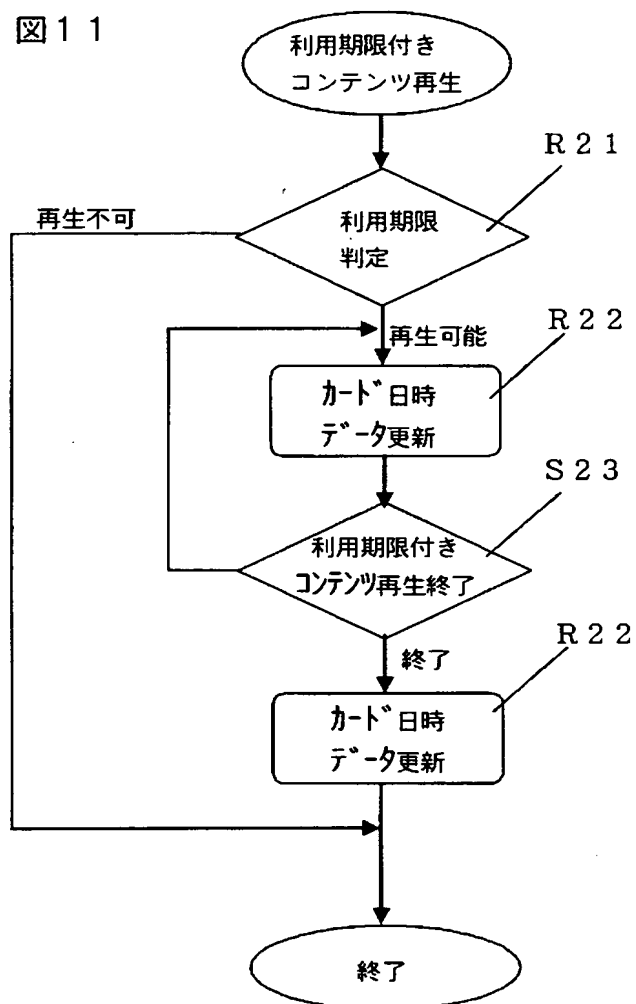
【図 10】

図 10



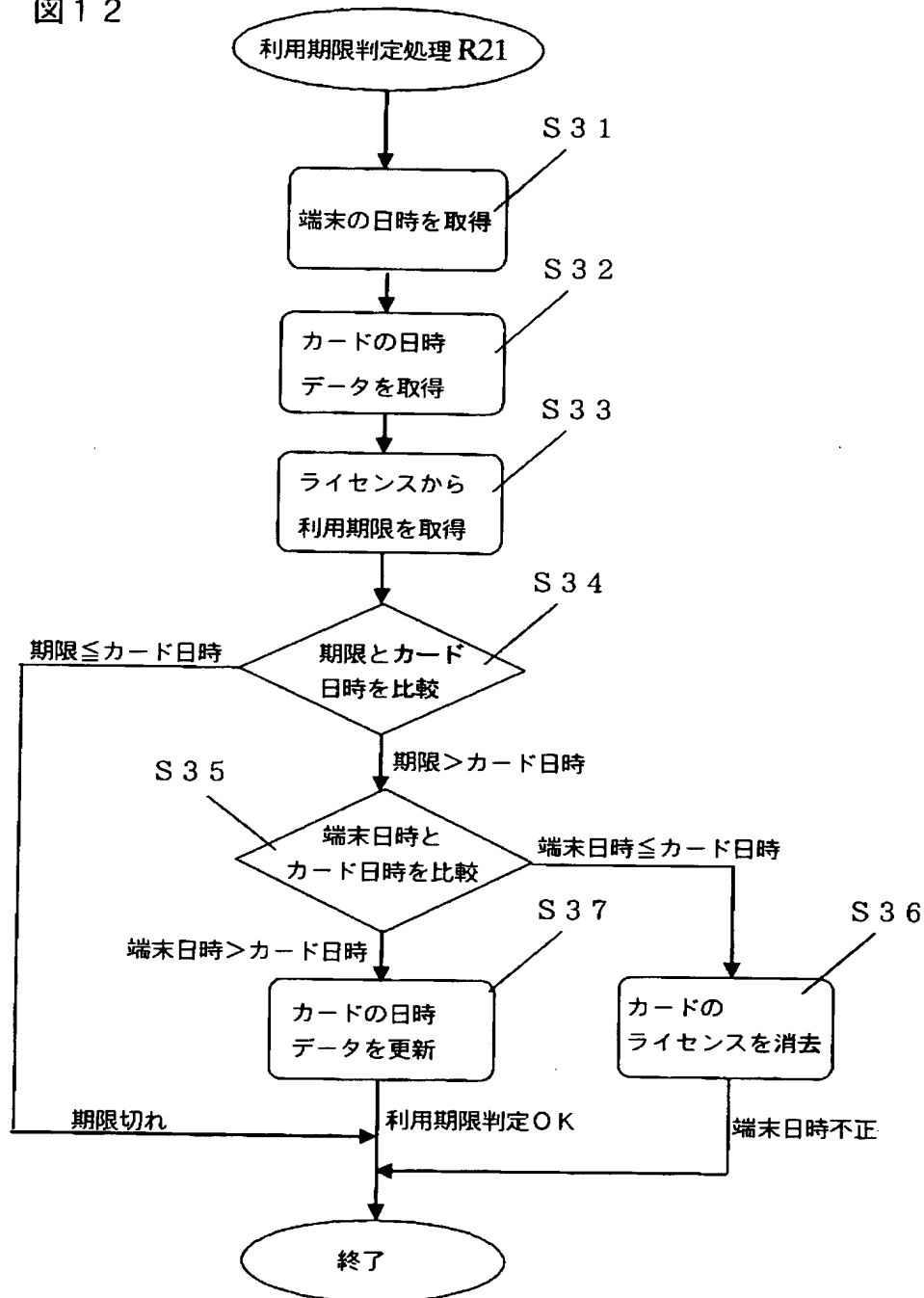
【図 11】

図 11



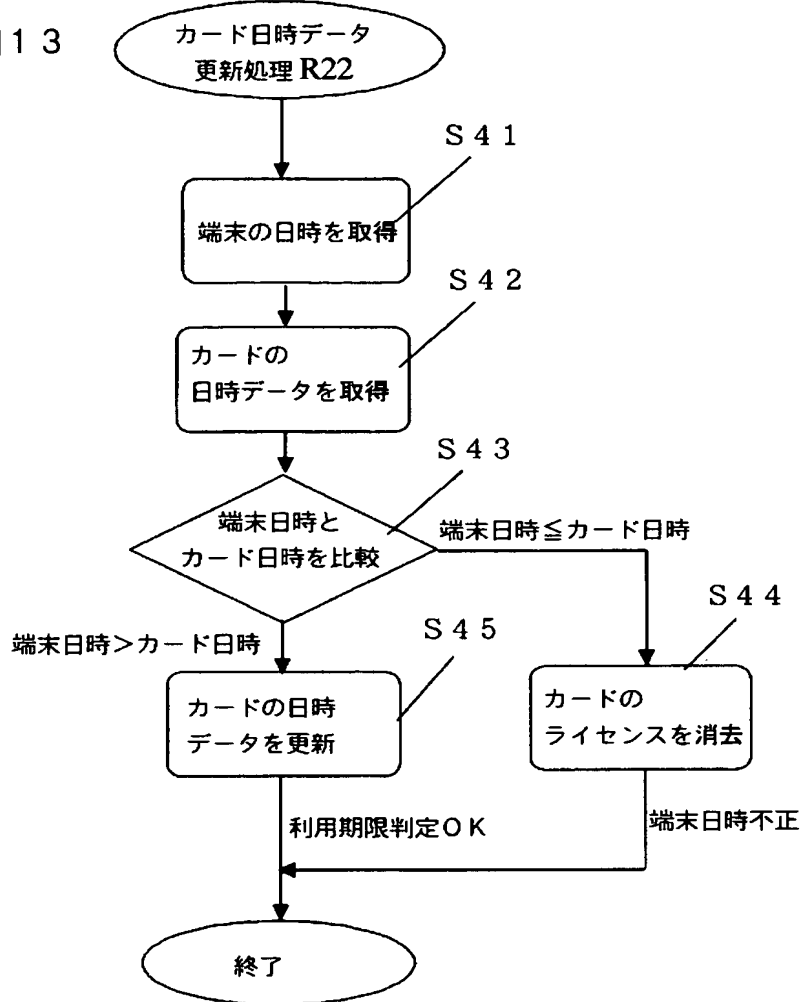
【図 12】

図 12



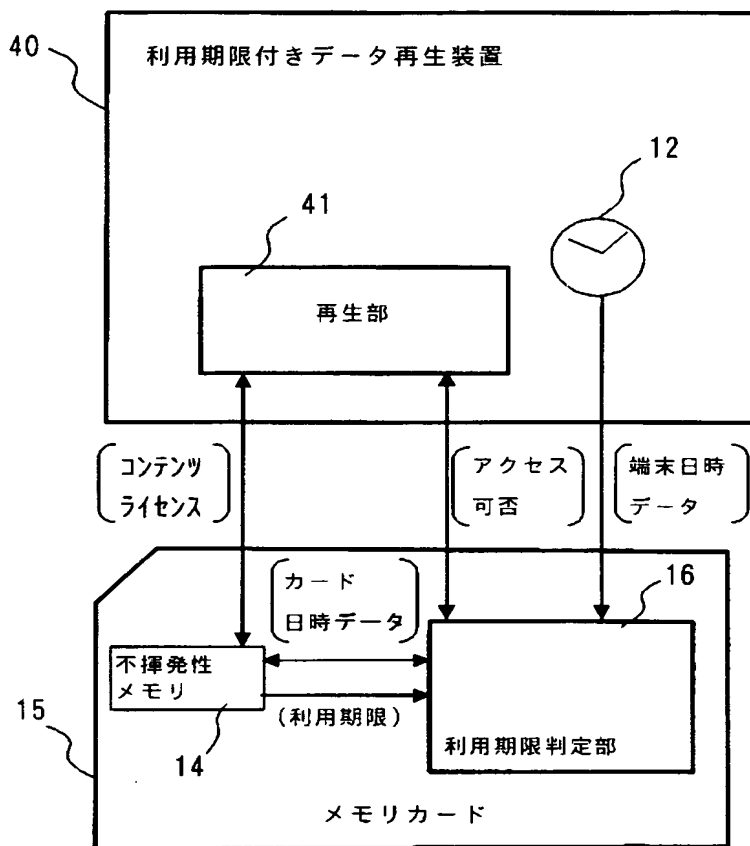
【図 13】

図 13



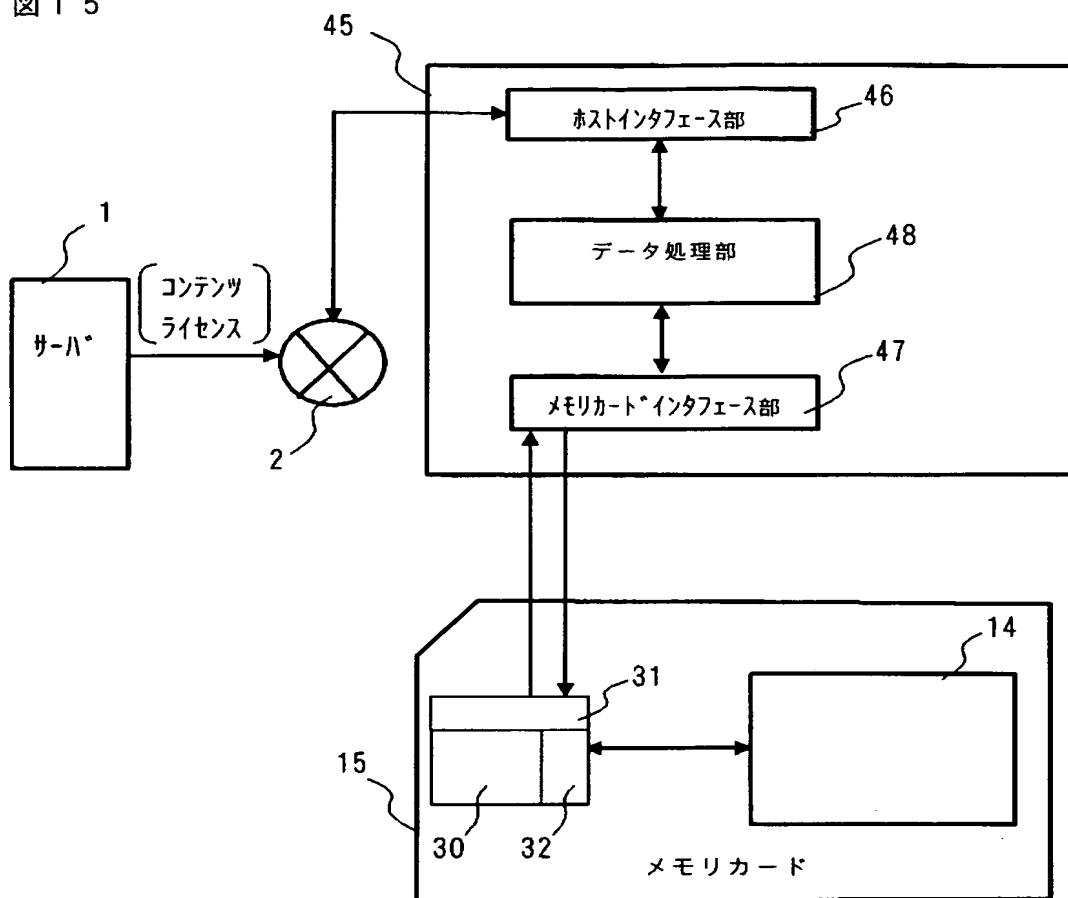
【図 14】

図 14



【図 15】

図 15



【書類名】 要約書

【要約】

【課題】 再生装置や端末装置内部の時計の操作による期限付きデータの不正アクセスを効果的に抑制する。

【解決手段】 不揮発性記憶装置は、制御回路（16）と不揮発性記憶回路（14）とを有する。不揮発性記憶回路は利用情報に対するアクセス制限を行なう制限情報の格納領域を有する。制限情報にはアクセス期限情報とアクセス時間情報とを含む。制御回路は、外部より供給される時刻情報と前記制限情報とに基いて利用情報のアクセス可否を判定し、時刻情報に基づいてアクセス時間情報を更新するアクセス判定動作を行なう。アクセス可否の判定において時刻情報がアクセス期限情報により示されるアクセス期限よりも後であり、又は時刻情報がアクセス時間情報により示されるアクセス時間よりも前である場合にアクセス否とする。アクセス判定動作を少なくとも前記利用情報に対するアクセス開始時とアクセス終了時とに行なう。

【選択図】 図2

特願 2 0 0 3 - 1 1 7 8 2 2

出 願 人 履 歴 情 報

識別番号

[5 0 3 1 2 1 1 0 3]

1. 変更年月日

2 0 0 3 年 4 月 1 日

[変更理由]

新規登録

住 所

東京都千代田区丸の内二丁目 4 番 1 号

氏 名

株式会社ルネサステクノロジ

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.